



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/827,227	04/05/2001	Philip D. MacKenzie	9	6212
7590	04/28/2005		EXAMINER	
Ryan, Mason & Lewis, LLP 90 Forest Avenue Locust Valley, NY 11560			MOORTHY, ARAVIND K	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/827,227	MACKENZIE, PHILIP D.
Examiner	Art Unit	
Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 07 April 2005.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-20 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 09 July 2001 is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____

DETAILED ACTION

1. This is in response to the amendment filed on 7 April 2005.
2. Claims 1-20 are pending in the application.
3. Claims 1-20 are allowable over prior art.

Response to Arguments

4. Applicant's arguments, see pages 2-4, filed 7 April 2005, with respect to claims 1-20 have been fully considered and are persuasive. The art rejection of the claims has been withdrawn.

Double Patenting

5. **Claims 1 and 3-8 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-6 and 18 of copending Application No. 09/638320 in view of Schneier (Applied Cryptography).**

Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims of the immediate application have all of the limitations of the copending application's claims. The dependent claims are identical. The independent claims of the immediate application, 1 and 8, only differ in that they add the limitation "wherein any portion of a result associated with the function that is outside the group is randomized" and the limitation "remove the randomization of any portion of the result associated with the function that is outside the group". All of the other limitations are claimed in the copending application. Schneier (Applied Cryptography) teaches a method of key authenticating as disclosed in the copending application. Schneier also teaches randomizing the result on page 520 to strengthen the security of the cryptosystem. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the

copending application's system because it would prevent possible attacks to the system by further disguising the random numbers. It logically follows that the receiver must then remove the randomized portion to recover the intended data.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

6. Claims 10 and 12-16 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-6 of copending Application No. 09/638320.

The rejection is similar to the double patenting rejection made of immediate claims 1 and 3-7, the difference being that independent claim 10 disclosed an apparatus which performs the method of claim 1. One of ordinary skill in the art would be able to implement the method of claim one as an apparatus.

7. Claims 17 is provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 18 of copending Application No. 09/638320.

The rejection is similar to the double patenting rejection made of immediate claims 8, the difference being that independent claim 17 disclosed an apparatus which performs the method of claim 1. One of ordinary skill in the art would be able to implement the method of claim one as an apparatus.

8. Claims 19 and 20 are likewise rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 and 18 of copending Application No. 09/638320.

The rejection is similar to the double patenting rejection made of immediate claims 1 and 8, the difference being that independent claims 19 and 20 disclosed an article of manufacture, which performs the method of claims 1 and 8. One of ordinary skill in the art would be able to implement the method of claim one as an article of manufacture.

Allowable Subject Matter

9. Claims 1-20 are allowed.

As to claims 1, 10, and 19, prior art does not disclose, teach or fairly suggest a method for communication via a data network, between two parties that share a password, using a Diffie-Hellman type key exchange on a particular group to generate a shared secret g^{xy} , where g is the group generator known to both parties and x is an index known to one party and y is an index known to the other party, said group having a group operation and an inverse group operation. Prior art does not disclose, teach or fairly suggest one party generating a parameter m by performing the group operation on g^x and a function of at least said password. Prior art does not disclose, teach or fairly suggest that any portion of a result associated with the function that is outside the group is randomized and transmitting m to the other party. Prior art does not disclose, teach or fairly suggest that the other party may perform the inverse group operation on m and said function of at least said password and remove the randomization of any portion of the result associated with the function that is outside the group, to extract g^x and further calculate said shared secret g^{xy} .

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy 
April 18, 2005


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100